

1 COOLEY LLP
2 MATTHEW D. BROWN (196972)
3 (brownmd@cooley.com)
4 REECE TREVOR (316685)
5 (rtrevor@cooley.com)
6 3 Embarcadero Center, 20th Floor
7 San Francisco, California 94111-4004
8 Telephone: +1 415 693 2000
9 Facsimile: +1 415 693 2222

10 Attorneys for SHOTSPOTTER, INC.

11
12 UNITED STATES DISTRICT COURT
13 NORTHERN DISTRICT OF CALIFORNIA
14
15 SAN FRANCISCO DIVISION
16

17 UNITED STATES OF AMERICA,
18
19 Plaintiff,
20
21 v.
22
23 JASON LEE,
24
25 Defendant.
26
27
28

Case No. 21-CR-00289-CRB

**THIRD-PARTY SUBPOENA RECIPIENT
SHOTSPOTTER, INC.'S MOTION FOR
PROTECTIVE ORDER**

Date: March 23, 2022
Time: 1:30 pm

NOTICE OF MOTION & MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD: PLEASE TAKE NOTICE THAT, on March 23, 2022 in Courtroom 6 of the above-captioned Court, third-party subpoena recipient ShotSpotter, Inc. will and hereby does move this Court, pursuant to Criminal Local Rule 17-2(c), for a protective order governing a document produced in response to a subpoena *duces tecum* to ShotSpotter.¹ This Motion is based upon the below Memorandum of Points and Authorities, the accompanying Declarations of Paul Greene and Matthew D. Brown, all papers on file in this action, and such other and further argument that the Court may consider.

STATEMENT OF RELIEF SOUGHT

ShotSpotter seeks a protective order governing the use and disclosure of a single confidential document provided to the Court in response to its February 11, 2022 subpoena to ShotSpotter.

STATEMENT OF ISSUES TO BE DECIDED

Whether there is good cause to limit a confidential ShotSpotter document's use to the parties in this matter and to prohibit its disclosure to the public on grounds in order to protect public safety and ShotSpotter's trade secrets.

MEMORANDUM OF POINTS AND AUTHORITIES

ShotSpotter respectfully requests that this Court enter a protective order limiting the disclosure of a single confidential ShotSpotter document to the parties in this action. This document contains sensitive information regarding ShotSpotter's processes for the forensic analysis of noise events, and it shows the locations of ShotSpotter sensors in several cities across the United States. Because public disclosure of this document would pose significant risks to public safety, to ShotSpotter's ability to reliably detect gunfire, and to ShotSpotter's interests in preserving its trade secrets, good cause exists for entry of a protective order.

¹ March 23, 2022 is the first hearing date available under Criminal Local Rule 47-2 and this Court's criminal law and motion calendar. However, because trial in this action is scheduled to begin before that day, ShotSpotter does not oppose an expedited briefing schedule, hearing date, or ruling. ShotSpotter in no way intends for this motion to delay the parties' access to the document at issue or to obstruct their preparation for trial.

1 This Court issued a subpoena *duces tecum* to ShotSpotter, which is not a party to this action,
 2 on February 11, 2022, and ShotSpotter has fully responded to that subpoena. As part of its response,
 3 ShotSpotter provided to the Court a document titled *ShotSpotter Browser* (the “Confidential
 4 Document”), which describes the ShotSpotter Browser software that the company’s forensic
 5 analysts use to perform multilateration calculations for use in litigation. Brown Decl. ¶ 2; Greene
 6 Decl. ¶ 7; *see also* SSTI_LEE_0000057-0081, delivered to the Court on February 28, 2022.

7 This software and its use are proprietary to ShotSpotter. Greene Decl. ¶¶ 7-9. Both the
 8 techniques used and the software itself were developed over the company’s many years of
 9 operation, drawing on its considerable expertise in the field of gunshot detection and analysis.
 10 Greene Decl. ¶¶ 8-9. As a result, the information reflected in the Confidential Document is of great
 11 economic significance to ShotSpotter, and its disclosure to competitors and potential competitors
 12 could undermine ShotSpotter’s hard-won advantage in this field. Greene Decl. ¶¶ 4, 9. ShotSpotter
 13 therefore takes reasonable measures to keep the Confidential Document and the locations of its
 14 sensors confidential, including by requiring its employees to execute nondisclosure agreements and
 15 by implementing various physical and electronic security measures. Greene Decl. ¶ 9. The
 16 Confidential Document accordingly constitutes a trade secret. *See* 18 U.S.C. § 1839(3) (defining a
 17 trade secret as “all forms and types of financial, business, scientific, technical, economic, or
 18 engineering information whose owner “derives independent economic value, actual or potential,
 19 from not being generally known to, and not being readily ascertainable through proper means by,
 20 another person” and “has taken reasonable measures to keep such information secret”).

21 Moreover, as part of its description of the ShotSpotter Browser software, the Confidential
 22 Document includes multiple screenshots that indicate the locations of ShotSpotter sensors in New
 23 York City, Oakland, and other jurisdictions (none of which pertain to San Francisco or the sensors
 24 involved in this case). Greene Decl. ¶ 14. The locations of ShotSpotter sensors, which are placed
 25 on private homes and businesses as well as on public property, are highly confidential. Greene
 26 Decl. ¶¶ 10, 13-14. Even ShotSpotter’s law enforcement agency clients generally do not know the
 27 detailed locations of sensors in the company’s network. Greene Decl. ¶ 13. With good reason—
 28 disclosure of these sensors would jeopardize the integrity of the sensors, the safety of those who

1 host them, and law enforcement’s ability to use ShotSpotter’s technology to respond to and
 2 investigate gunfire. Prior experience shows that when members of the public learn these sensors’
 3 locations, the consequences can be severe. Criminals seeking to evade ShotSpotter may deliberately
 4 damage or destroy the sensors. Greene Decl. ¶ 12. Worse still, community members who have
 5 agreed to host ShotSpotter sensors have received threats after their identities became public. *Id.*
 6 When sensors are disabled or third parties believe that working with ShotSpotter could endanger
 7 them, ShotSpotter’s ability to detect gunfire, assist law enforcement, and protect public safety
 8 suffers. Greene Decl. ¶¶ 11-13.

9 To safeguard these important community safety interests and ShotSpotter’s privacy
 10 interests, the Court should issue a protective order for the Confidential Document. Criminal Local
 11 Rule 17-2(c) specifically authorizes “an order to permit production” in response to a third-party
 12 subpoena “only pursuant to a protective order.” While the local rules do not provide a standard for
 13 evaluating such a motion, the Confidential Document easily satisfies the analogous “good cause”
 14 standard for protective orders governing discovery between the parties. Fed. R. Crim. P. 16(d)(1).
 15 Courts routinely grant protective orders for documents that “contain confidential financial, and
 16 other sensitive personal information.” *United States v. Smith*, No. 2:18-CR-133-RMP, 2018 U.S.
 17 Dist. LEXIS 140963, at *2 (E.D. Wash. Aug. 20, 2018). Indeed, this Court’s model protective
 18 order, on which ShotSpotter’s proposed order is based, envisions that the order may be “tailor[ed]”
 19 to provide “robust protections” for “trade secrets” like the Confidential Document or “cases in
 20 which exposure of protected material could endanger” individuals’ safety, as the revelation of
 21 ShotSpotter’s sensor locations might. N.D. Cal. Model Protective Order for Non-Complex Criminal
 22 Cases at 1 n.1.

23 Furthermore, ShotSpotter’s proposed order is narrowly tailored and allows the parties full
 24 use of the Confidential Document in litigating this action. ShotSpotter seeks protection for only a
 25 single document among the entirety of its subpoena response. Its proposed protective order would
 26 allow the defense and the United States to freely use the Confidential Document with their expert
 27 witnesses, assistants, consultants, and other members of their teams who would reasonably require
 28 access to the document. Consistent with the Northern District’s model protective order,

ShotSpotter's proposal would simply prohibit the litigants from sharing the Confidential Document with other parties and would require its return to ShotSpotter at the conclusion of the proceedings against Defendant and any action he may bring under 28 U.S.C. § 2255.

Prior to filing this Motion, ShotSpotter's counsel contacted counsel for the parties to seek a stipulation as to the protective order's scope and terms. Counsel for the United States indicated that they take no position on the protective order. Brown Decl. ¶¶ 3, 6. Even after several rounds of negotiation, ShotSpotter was unable to reach an agreement with defense counsel. *Id.* ¶ 4-6. ShotSpotter agreed to incorporate a number of changes designed to address the defense's concerns.² For instance, ShotSpotter included a provision that permits counsel to retain an archival copy of all pleadings, memoranda, and other work product even if it contains confidential information. *Id.* ¶ 4. ShotSpotter's proposed protective order here incorporates all of these changes. *Id.*

For all of the foregoing reasons, the Court should grant ShotSpotter's motion and issue its proposed protective order.

Dated: March 3, 2022

COOLEY LLP

By: /s/ Matthew D. Brown
Matthew D. Brown

Attorneys for SHOTSPOTTER, INC.

265062651

² Most saliently, defense counsel objected to a provision that required notice to ShotSpotter before the Confidential Document may be disclosed to persons associated with ShotSpotter's competitors, asserting that this provision intruded on Defendant's constitutional rights. Brown Decl. ¶ 5. As ShotSpotter's counsel noted to defense counsel, this provision does not prohibit such persons from accessing the Confidential Document in the first instance, but rather provides ShotSpotter with an opportunity to request that the Court's intervention if needed, and so implicates no constitutional concerns.